Appl. No. 10/799,316
Amdt. dated March 18, 2008
Reply to Office Action of November 23, 2007

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Please cancel claims 15-19 without prejudice and amend claims 1-8 as follows:

1. (amended) A method for Galois field ($GF(2^m)$) multiplication, where m is a positive integer, and the $GF(2^m)$ multiplication operation calculates the multiplication of two polynomials producing a product which is divided by a generator polynomial, and wherein the multiplication ~~operation~~ of the two polynomials is ~~further~~ combined with the division operation whereby the $GF(2^m)$ multiplication ~~may be~~ is computed ~~in~~ as a single ~~logic stage~~ function $GF(2^m)$ multiplication operation, the method comprising:

generating x^{m-i} polynomial coefficient terms from multiplication and division mathematical operations, where i is a variable;

combining ~~like~~ x^{m-i} polynomial coefficient terms having the same exponents from the multiplication and division mathematical operations to generate a recurrence relation that represents the combination of the multiplication and division operations; ~~and~~

computing ~~a~~ the recurrence relation using the combined x^{m-i} polynomial coefficient terms ~~for~~ in the single function $GF(2^m)$ multiplication ~~function~~ operation to produce a $GF(2^m)$ result; and

storing the $GF(2^m)$ result in memory in a computer readable form.

2. (amended) The method of claim 1 wherein the recurrence relation for ~~a~~ the single $GF(2^m)$ multiplication function is $Y(i) = Y(i-1) + (q_{m-i}*p + Y(i-1)_{2m-1}*g)*x^{m-i}$, $i=1, 2, \ldots, m$ and where $Y(0) = 0$, $Y(i=m)$ is the $GF(2^m)$ result, p and q are coefficients of input polynomials p[x] and q[x], respectively, and g is the coefficients of a generator polynomial g[x].

3. (amended) The method of claim 1 further comprising:

computing the recurrence relation for a single $GF(2^m)$ multiplication function as $Y(i) = Y(i-1) + (q_{m-i}*p + Y(i-1)_{2m-1}*g\ Y(i-1)_{m-1}*g)*x^{m-i}$, $i=1, 2, \ldots, m$ and where $Y(0) = 0$, $Y(i=m)$ is the $GF(2^m)$ result, p and q are coefficients of input polynomials p[x] and q[x], respectively, and g is the coefficients of a generator polynomial g[x] in an m by m single function computation array utilizing m bits per internal calculation stage

~~outputting results from computing the recurrence relation; and~~

~~storing the results in computer readable form~~.

4. (amended) A method for Galois field ($GF(2^m)$) multiplication, where m is a positive integer, and the $GF(2^m)$ multiplication operation calculates the multiplication of two polynomials producing a product which is divided by a generator polynomial, and wherein the multiplication ~~operation~~ of the two polynomials is ~~further~~ combined with the division operation whereby the $GF(2^m)$ multiplication ~~may be~~ is computed ~~in~~ as a single ~~logic stage~~ function $GF(2^m)$ multiplication operation, the method comprising:

generating x^{m-i} polynomial coefficient terms from multiplication and division mathematical operations, where i is a variable;

combining ~~like~~ x^{m-i} polynomial coefficient terms having the same exponents from the multiplication and division mathematical operations to generate a recurrence relation that represents the combination of the multiplication and division operations; ~~and~~

computing ~~a~~ the ~~simplified~~ recurrence relation using the combined x^{m-i} polynomial coefficient terms ~~for~~ in the single function GF(2^m) multiplication ~~function~~ operation thereby calculating m by m bits for the ~~simplified~~ GF(2^m) multiplication function to produce an m bit GF(2^m) result; and

storing the m bit GF(2^m) result in memory in a computer readable form.

5. (amended) The method claim 4 wherein the ~~simplified~~ the recurrence relation for the single GF(2^m) multiplication function is $Y(i) = Y(i-1) + (q_{m-i}*p + Y(i-1)_{m-1}*g)*x^{m-i}$, i=1, 2, …, m and where Y(0) = 0, Y(i=m) is the m bit GF(2^m) result, p and q are coefficients of input polynomials p[x] and q[x], respectively, and g is the coefficients of a generator polynomial g[x].

6. (amended) The method of claim 4 ~~further comprising:~~ wherein the step of computing the recurrence relation is accomplished in an m by m single function computation logic array utilizing m bits per internal logic stage

~~outputting results from computing the simplified recurrence relation; and~~

~~storing the results in computer readable form~~.

7. (amended) A GF multiplication circuit cell producing result $Y(i)_j$ for $i \in \{1, 2, \ldots, m\}$, $j \in \{0, 1, \ldots, m-1\}$, where m is a positive integer, and a selected i and j value comprising:

a bit q_{m-i} selected from the set $\{q_{m-1}, q_{m-2}, \ldots, q_{m-i}, \ldots, q_0\}$ of first product inputs based on the selected i value;

a bit p_j selected from the set $\{p_{m-1}, p_{m-2}, \ldots, p_j, \ldots, p_0\}$ of second product inputs based on the selected j value;

a bit g_j selected from the set $\{g_{m-1}, g_{m-2}, \ldots, g_j, \ldots, g_0\}$ of generator polynomial coefficients based on the selected j value;

~~the~~ a most significant bit $Y(i-1)_{m-1}$ of ~~the~~ a previous stage of GF multiplication circuit cells ~~values~~ results;

~~the~~ a value of the rightmost neighbor bit $Y(i-1)_{j-1}$ of a previous stage of GF multiplication circuit cell results, wherein the rightmost neighbor bit $Y(i-1)_{j-1}$ is in relation to the present GF multiplication circuit cell producing result $Y(i)_j$ for the selected i and j values;

a logic device producing q_{m-i} AND p_j as output A;

a logic device producing $Y(i-1)_{m-1}$ AND g_j as output B; and

a logic device producing A XOR B XOR $Y(i-1)_{j-1}$ as ~~output~~ result $Y(i)_j$ to be utilized in one or more GF multiplication circuit cells or stored in a processor accessible storage unit.

8. (amended) The GF multiplication circuit cell of claim 7 disposed within an m-by-m array of interconnected GF multiplication circuit cells for producing a Galois Field (2^m) multiplication result Y, where m is a positive integer, further comprising:

input operand $q = (q_{m-1}\ q_{m-2}\ \ldots\ q_0)$;

input operand $p = (p_{m-1}\ p_{m-2}\ \ldots\ p_0)$;

input operand $g = (g_{m-1}\ g_{m-2}\ \ldots\ g_0)$;

the $Y(i-1)_{m-1}$ and the $Y(i-1)_{j-1}$ array border GF multiplication circuit cell input values set to 0; and

output Y result[[s]] which is stored in a computer readable form~~; and~~

~~an m-by-m array of interconnected GF multiplication circuit cells~~.

9. (original) The GF multiplication circuit cell of claim 8 wherein the m-by-m array of interconnected GF multiplication circuit cells further comprises:

the interconnections of the GF multiplication circuit cells governed by the equation $Y(i) = Y(i\text{-}1) + (q_{m\text{-}i}*p + Y(i\text{-}1)_{m\text{-}1}*g)*x^{m\text{-}i}$, $i=1, 2, \ldots, m$ and where $Y(0) = 0$.

10. (original) The GF multiplication circuit cell of claim 8 wherein the m-by-m array of GF multiplication circuit cells is further disposed within a grouping of multiple m-by-m arrays in a processor execution unit and further comprises:

a GF (2^m) multiplication instruction with a data type field specifying at least one GF (2^m) multiplication operation; and

means for connecting the multiple m-by-m arrays inputs and outputs for performing at least one GF (2^m) multiplication in the execution of the GF (2^m) multiplication instruction.

11. (original) The GF multiplication circuit cell of claim 8 wherein the input operands $q = (q_{m\text{-}1}\ q_{m\text{-}2} \ldots q_0)$, $p = (p_{m\text{-}1}\ p_{m\text{-}2} \ldots p_0)$, and $g = (g_{m\text{-}1}\ g_{m\text{-}2} \ldots g_0)$ are connected to read outputs of at least one storage unit in a processor system.

12. (original) The GF multiplication circuit cell of claim 8 wherein the output Y results are connected to at least one storage unit write inputs in a processor system.

13. (original) The GF multiplication circuit cell of claim 11 wherein the at least one storage unit is a processor accessible register file.

14. (original) The GF multiplication circuit cell of claim 12 wherein the at least one storage unit is a processor accessible register file.

15-19. (canceled)